Elektrobit

UDACITY

Safety Plan Lane Assistance

Document version: 0.1

Template version: 1.0, Released on 2017-06-21

Author:
Konstantin Selyunin

August 23, 2018

Revision History

Version	Date	Editor	Description
0.1	2018/08/13	Konstantin Selyunin	LaTeX template created
0.2	2018/08/19	Konstantin Selyunin	Filling the content part

Contents

1 Introduction

1.1 Purpose of the Safety Plan

The safety plan serves as a guide and provides a framework for achieving the functional safety. It also defines roles and responsibilities between the project parties. This document presents a safety plan for a Lane assistance item, in order to achieve functional safety defined in the standard [1].

1.2 Scope of the Project

For the lane assistance project, the following safety lifecycle phases are in scope:

- Concept phase
- Product Development at the System Level
- Product Development at the Software Level

The following phases are out of scope:

- Product Development at the Hardware Level
- Production and Operation

1.3 Deliverables of the Project

The deliverables of the project are:

- Safety Plan
- Hazard Analysis and Risk Assessment
- Functional Safety Concept
- Technical Safety Concept
- Software Safety Requirements and Architecture

2 Item definition

The item in question is the Lane Assitance system, with the purpose to assist the driver in staying in the lane, and notifying the driver if a car is leaving the lane.

The Lane Assistance System has two functions:

1. Lane departure warning
2. Lane keeping assistance

"The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback": whenever a car is about to leave the lane where the car is currently driving, a steering wheel vibrates and alerts the driver about this situation.

"The lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane": i.e. the lane keeping assistance steers the vehicle towards the center of the current driven lane.

The lane assistance system consists of the following sub-systems (Fig. 2.1):

- Camera sub-system;
- Electronic Power Steering sub-system;
- Car Display sub-system.

A camera sub-system is responsible for detecting position of the car w.r.t. to the center of the ego lane and w.r.t. to the road and sending a torque request.

An electronic power steering ECU is responsible for receiving a torque request and activating a motor providing torque request to the steering wheel.

A car display sub-system is used to warn a driver about mal-function of the system.

The item boundaries are illustrated in Figure 2.2:

As seen from the Figure 2.2 the steering wheel is outside the Lane Assistance Item. It is also implied that the engine, the breaking item are outside the Lane Assistance Item.

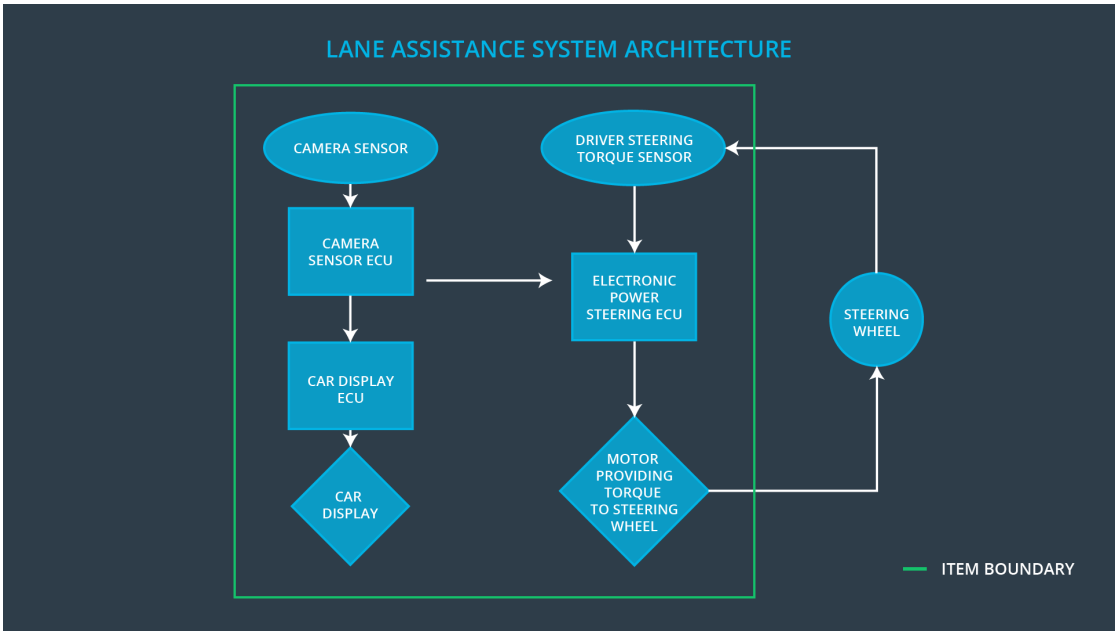

Figure 2.1: Lane assistance system architecture

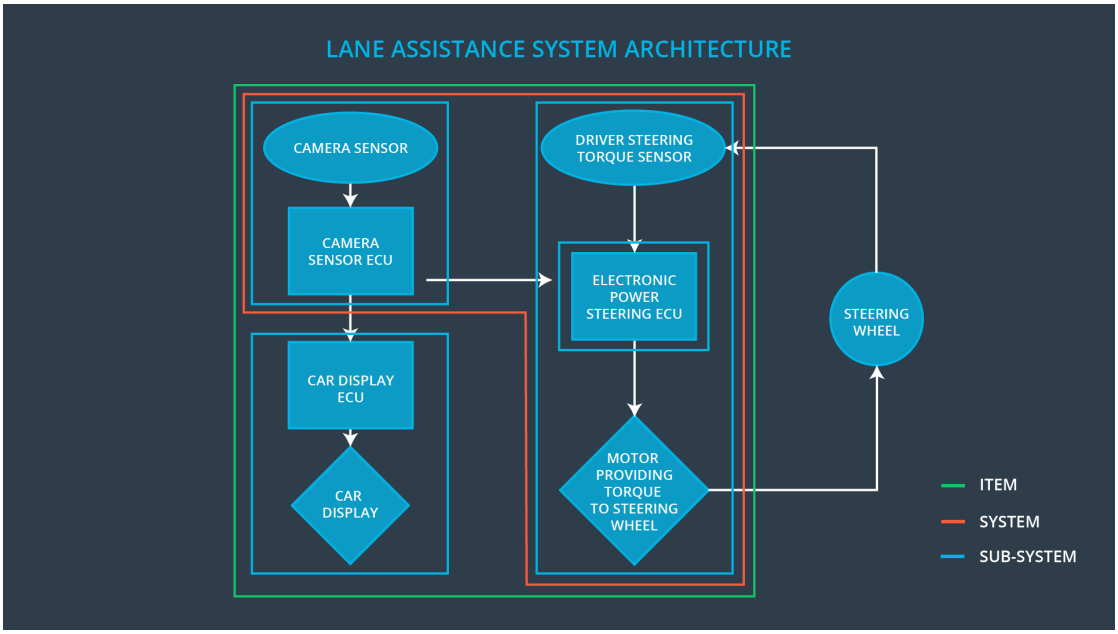

Figure 2.2: Boundaries of the Lane assistance system and its sub-systems

3 Goals and Measures

3.1 Goals

The goal of the project is to identify functional safety requirements, safety goals and propose means to achieve these safety goals using system's engineering.

In general, this is done by identifying hazardous situations, and finding ways to reduce the risk of these hazards to the levels acceptable by society.

By analyzing the Lane Assistance function with ISO 26262 we are trying to come up with the design of a system, using means and guidelines provided by the standard, such that the system is safe for humans to use, and would not create unnecessary dangerous situation, while using the system.

The goal of this project can then be summarized as follows:

1. Identify hazards in a Lane Assistance item that could cause physical injury or damage to a person's health
2. Evaluate the risk of the hazardous situation
3. Using systems engineering, propose means to prevent accidents from occurring by lowering risk to reasonable levels.

3.2 Measures

Table 3.1 defines the following measures to maintain the safety standard defined by the ISO 26262.

The key team members in the Lane Assistance project and their the main responsibilities are as follows:

1. Project Manager
    - Overall project management
    - Acquires and allocates resources needed for the functional safety activities
    - Appoints safety manager or might act as safety manager
2. Safety Manager
    - Planning, coordinating and documenting of the development phase of the safety lifecycle

Table 3.1: Responsibilities for measures & activities

Measures and Activities	Responsibility	Timeline
Follow safety processes	All Team Members	Constantly
Create and sustain a safety culture	Safety Manager, All Team Members	Constantly
Coordinate and document the planned safety activities	Safety Manager	Constantly
Allocate resources with adequate functional safety competency	Project Manager	Within 2 weeks of start of project
Tailor the safety lifecycle	Safety Manager	Within 4 weeks of start of project
Plan the safety activities of the safety lifecycle	Safety Manager	Within 4 weeks of start of project
Perform regular functional safety audits	Safety Manager	Once every 2 months
Perform functional safety pre-assessment prior to audit by external functional safety assessor	Safety Auditor	3 months prior to main assessment
Perform functional safety assessment	Safety Assessor	Conclusion of functional safety activities

- Tailors the safety lifecycle
- Maintains the safety plan
- Monitors progress against the safety plan
- Performs pre-audits before the safety auditor

3. Safety Engineer
    - Product development
    - Integration
    - Testing at the hardware, software and system levels
4. Safety Auditor
    - Ensures that the design and production implementation conform to the safety plan and ISO 26262.
    - Must be independent from the team developing the project
5. Safety Assessor
    - Independent judgement as to whether functional safety is being achieved via a functional safety assessment

- Must be independent from the team developing the project

6. Test Manager
    - Plans testing activities
    - Coordinates testing to show that the vehicle system works correctly

4 Safety Culture

To support development, production, and integration of safe systems, we put safety the highest priority over competing constraints (e.g. cost, productivity), and promote the following safety principles:

- **High priority:** safety has the highest priority among competing constraints like cost and productivity
- **Accountability:** our processes ensure accountability such that design decisions are traceable back to the people and teams who made the decisions
- **Rewards:** our organization motivates and supports the achievement of functional safety
- **Penalties:** our organization penalizes shortcuts that jeopardize safety or quality
- **Independence:** design teams are independent from the teams who audit the work
- **Well defined processes:** our company clearly defines design and management processes
- **Resources:** projects have necessary resources including people with appropriate skills
- **Diversity:** intellectual diversity is sought after, valued and integrated into processes
- **Communication:** communication channels encourage disclosure of problems

Our Organization has a quality management system in place that complies with quality management standards IATF 16949.

5 Safety Lifecycle Tailoring

In this project, the following safety lifecycle phases are in scope:

- **Concept phase:** defining the safety concept and the corresponding safety requirements
- **Product Development at the System Level:** identifying functional components of the system with a dedicated functionality boundaries between these components
- **Product Development at the Software Level:** defining the software components of the system with, defining the functionality of these components and means of interactions between the components.

The following phases are out of scope:

- **Product Development at the Hardware Level:** defining hardware components, parts selection, PCB design, hardware communication interfaces
- **Production and Operation** identifying how the product should be maintained during use

6 Roles

The Table 6.1 presents roles involved in the functional safety project and where they belong (OEM, Tier-1 or External).

Table 6.1: Roles

Role	Org
Functional Safety Manager - Item Level	OEM
Functional Safety Engineer - Item Level	OEM
Project Manager - Item Level	OEM
Functional Safety Manager- Component Level	Tier-1
Functional Safety Engineer- Component Level	Tier-1
Functional Safety Auditor	OEM or external
Functional Safety Assessor	OEM or external

7 Development Interface Agreement

The purpose of a development interface agreement (DIA) is to define the roles and responsibilities between companies involved in developing a Lane Assistance Item. In addition, it serves as a written agreement between the parties involved in the project. The DIA also specifies the evidence and outcomes each party in order to justify the correct and transparent execution of the agreement.

In this project the OEM is supplying a functioning lane assistance system. Our company needs to analyze the software components of the EPS sub-system.

8 Confirmation Measures

8.1 Main purpose of the safety plan

The main purpose of the confirmation measures is to check the following:

- Processes comply with the functional safety standard
- Project execution is following the safety plan
- Design really does improve safety

8.2 Confirmation review

A confirmation review ensures that the project complies with ISO 26262. During the design and development of the lane assistance item an independent person would review the work to make sure ISO 26262 is being followed.

8.3 Functional Safety Audit

A functional safety audit performs checks to make sure that the actual implementation of the project conforms to the safety plan.

8.4 Functional Safety Assessment

A functional safety assessment aims to Confirm that plans, designs and developed lane assistance item actually achieve functional safety.

A safety plan could have other sections that we are not including here. For example, a safety plan would probably contain a complete project schedule.

There might also be a "Supporting Process Management" section that would cover "Part 8: Supporting Processes" of the ISO 26262 functional safety standard. This would include descriptions of how the company handles requirements management, change management, configuration management, documentation management, and software tool usage and confidence.

Similarly, a confirmation measures section would go into more detail about how each confirmation will be carried out.

9 List of Abbreviations

ISO	International Organization for Standardization
ASIL	Automotive Safety Integrity Level
ECU	Electronic Control Unit
EPS	Electronic Power Steering
OEM	Original Equipment Manufacturer

Bibliography

[1] Organización Internacional de Normalización. *ISO 26262: Road Vehicles : Functional Safety*. ISO, 2011.